(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
22 mars 2001 (22.03.2001)

PCT

(10) Numéro de publication internationale
WO 01/20870 A1

(51) Classification internationale des brevets[7]: H04L 29/06, 29/12

(21) Numéro de la demande internationale:
PCT/FR00/02469

(22) Date de dépôt international:
7 septembre 2000 (07.09.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/11594 16 septembre 1999 (16.09.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: **BULL S.A.** [FR/FR]; 68, route de Versailles, F-78430 Louveciennes (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)*: **DUJONC, Jean-Yves** [FR/FR]; 27 bis, avenue Pasteur, F-78580 Maule (FR). **MARTIN, René** [FR/FR]; 32, rue Gometz, F-91440 Bures sur Yvette (FR).

(74) Mandataire: **DENIS, Hervé**; Bull S.A., 68, route de Versailles, (P.C.: 58D20), F-78434 Louveciennes Cedex (FR).

(81) États désignés *(national)*: CN, JP, KR, SG, US, VN.

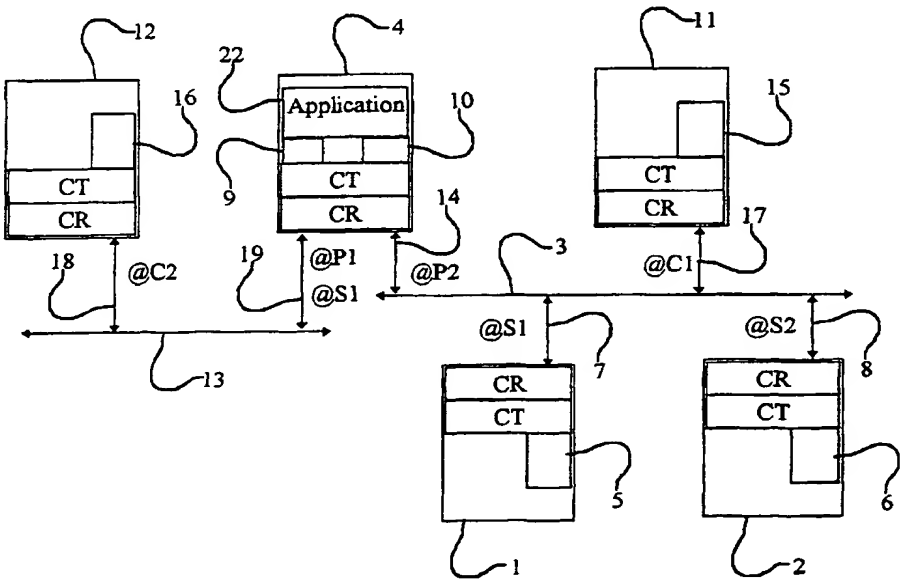
(84) États désignés *(régional)*: brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée:
— *Avec rapport de recherche internationale.*

[Suite sur la page suivante]

(54) Title: TRANSPARENT ACCESS RELAY TO A SERVER NETWORK

(54) Titre: RELAIS D'ACCES TRANSPARENT A UN RESEAU SERVEUR



(57) Abstract: The invention concerns an interconnection machine (4) connected to a client network (13) by a first physical interface (19) and connected to a server network (3) by a second physical interface (14). The interconnection machine (4) comprises a first relay application (22) for receiving datagrams addressed to the server machine (1, 2) from the network (13) and for transmitting on the network (3) datagrams addressed to the server machine (1, 2). An inter-network protocol address (@S1, @S2) of a server machine (1, 2) connected to the server network (3), is associated with the first physical interface (19) so that the datagrams routed to the applicative level in the interconnection machine are transparently available to the proxy on the client network (13).

[Suite sur la page suivante]

WO 01/20870 A1

En ce qui concerne les codes à deux lettres et autres abréviations. se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé:** L'invention concerne une machine d'interconnexion (4) reliée à un réseau client (13) au moyen d'une première interface physique (19) et reliée à un réseau serveur (3) au moyen d'une deuxième interface physique (14). La machine d'interconnexion (4) comprend une première application relais (22) pour recevoir des datagrammes destinés à la machine serveur (1, 2) depuis le réseau (13) et pour émettre sur le réseau (3) des datagrammes à destination de la machine serveur (1, 2). Une adresse protocolaire inter-réseaux (@S1, @S2) d'une machine serveur (1, 2) reliée au réseau serveur (3), est associée à la première interface physique (19) de sorte que les datagrammes remontant au niveau applicatif dans la machine d'interconnexion sont à disposition de l'application relais de façon transparente sur le réseau client (13).

RELAIS D'ACCES TRANSPARENT A UN RESEAU SERVEUR

Le domaine technique auquel se rapporte l'invention est celui des réseaux informatiques. Les réseaux informatiques permettent l'exécution d'applications réparties sur des machines distantes reliées à un même réseau ou reliées à des réseaux différents interconnectés au moyen de machines d'interconnexions.

Une transaction entre machines distantes est initiée par une application client qui émet un message de requête vers une application serveur en état de veille. L'application client se met en état d'attente d'un message de réponse à son message de requête. A réception du message de requête, l'application serveur élabore un message de réponse qu'elle émet vers l'application client. Une couche réseau permet de véhiculer chaque message sous forme de datagramme, depuis la machine qui héberge l'application émettrice jusqu'à la machine qui héberge l'application réceptrice. Une couche transport permet de véhiculer le message entre l'application émettrice et la couche réseau puis entre la couche réseau et l'application réceptrice, c'est à dire par exemple d'une application client à une application serveur. Une couche applicative concerne l'exécution de l'application dans l'environnement qui lui est propre.

Lorsque les machines ne sont pas physiquement liées au même réseau, des protocoles de routage de la couche réseau acheminent les datagrammes depuis la machine émettrice vers une machine d'interconnexion et de la machine d'interconnexion vers la machine réceptrice au moyen d'adresses protocolaire inter-réseaux telles que par exemple les adresses IP. Au passage dans la machine d'interconnexion, les datagrammes restent au niveau de la couche réseau. Le réseau entre la machine client et la machine d'interconnexion est appelé réseau client. Le réseau entre la machine serveur et la machine d'interconnexion est appelé réseau serveur.

Le domaine technique auquel se rapporte plus particulièrement l'invention concerne une machine d'interconnexion pour héberger une application relais (proxy en anglais). Une application relais est intéressante pour effectuer des traitements sur les messages échangés entre le réseau client et le réseau serveur. Cependant, les datagrammes destinés à la machine réceptrice finale ne sont pas naturellement remontés à la couche applicative de la machine d'interconnexion.

Selon l'état de la technique antérieure connu, l'application émettrice adresse ses messages à l'application relais de la machine d'interconnexion au lieu de les adresser directement à l'application réceptrice finale et indique dans ses messages à l'application relais à quelle application finale ses messages sont destinés de sorte que l'application relais puisse les y réacheminer en fonction de traitements qu'elle leur applique. C'est ce qu'on retrouve par exemple dans un navigateur internet (browser en anglais) où il est possible de déclarer pour une application client donnée, l'adresse de la machine d'interconnexion pour la couche réseau et le numéro de port de l'application relais pour la couche transport, de sorte que le navigateur encapsule l'adresse de la machine serveur et le numéro de port de l'application destinatrice finale dans un datagramme adressé à l'application relais. Cependant, cela nécessite de connaître par quelle application relais doivent passer les messages de façon à configurer la machine client en conséquence. Le manque de souplesse qui en résulte, s'il convient pour un nombre limité d'applications, n'est pas satisfaisant pour un grand nombres d'applications distinctes.

Le document RFC1928 disponible sur internet à l'adresse http://www.pmg.lcs.mit.edu/cgi-bin/rfc/view?1928 décrit le protocole "SOCKS v5" dont le numéro de port utilisé par convention est 1080. De la même façon que pour la solution connue sous le nom "TCP protocol Tunelling in Web Proxy Servers", il est nécessaire d'établir une première connexion vers l'application relais, suivie d'une deuxième connexion de la machine relais vers la machine finale.

Pour pallier les inconvénients précédemment cités, le but de l'invention est de permettre à une application client de simplement établir une connexion vers une application serveur comme elle le ferait sans utilisation des services d'une application relais, de sorte que l'utilisation des services de l'application relais est transparente pour l'application client.

Un premier objet de l'invention est une machine d'interconnexion reliée à un réseau client au moyen d'une première interface physique et reliée à un réseau serveur au moyen d'une deuxième interface physique, caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux d'une machine serveur reliée au réseau serveur, est associée à la première interface physique, et en ce qu'elle comprend une première application relais pour recevoir des datagrammes destinés à la machine serveur depuis le réseau client et pour émettre sur le réseau serveur des datagrammes à destination de la machine serveur.

Ainsi, lorsqu'un datagramme se présente sur la première interface physique avec l'adresse protocolaire inter-réseaux de la machine serveur comme adresse de destination, la machine d'interconnexion est reconnue par sa couche réseau comme étant la machine de destination du datagramme. La couche réseau de la machine d'interconnexion remonte alors le datagramme vers la couche applicative de la machine d'interconnexion par simple respect du protocole établi. Recevant ce datagramme, l'application relais peut le traiter puis le réemmettre ou ne pas le réémettre vers la machine serveur. Ceci est totalement transparent pour l'application client.

Une variante de l'invention a pour objet une machine d'interconnexion reliée à un réseau client au moyen d'une première interface physique et reliée à un réseau serveur au moyen d'une deuxième interface physique, caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux d'une machine serveur reliée au réseau serveur, est associée à une troisième interface physique, distincte de la première interface physique et de la deuxième interface physique et en ce qu'elle comprend une première application relais pour rec voir des datagrammes destinés à la machine serveur depuis le réseau client et pour émettre sur le réseau serveur des datagrammes à destination de la machine serveur.

Ici, le protocole de la couche réseau ne nécessite pas que l'adresse de destination soit affectée à la première interface physique qui reçoit le datagramme mais à une quelconque interface physique de la machine d'interconnexion, pour être remonté vers la couche applicative de la machine d'interconnexion.

Lorsque la machine d'interconnexion possède déjà une adresse de base sur le réseau client, utile par exemple à des protocoles de routage, ladite adresse de machine serveur est associée à la première interface physique en tant qu'adresse synonyme de l'adresse de base de la machine d'interconnexion sur le réseau client.

Un deuxième objet de l'invention est un procédé pour permettre de traiter au moyen d'une application relais exécutée dans une machine d'interconnexion entre un réseau client et un réseau serveur, des datagrammes émis sur le réseau client par une application client à destination d'une machine serveur possédant une adresse sur le réseau serveur, caractérisé en ce qu'il comprend une première étape qui associe ladite adresse sur le réseau serv ur à une interface physique de la machine d'interconnexion qui n'est pas reliée au réseau serveur, de sorte que l'application relais capte les dits datagrammes.

Ceci présente l'avantage de ne pas nécessiter de configurer ou d'informer ladite application client pour que l'application relais puisse traiter les datagrammes. En effet, l'application client continue à émettre ses datagrammes en utilisant l'adresse de la machine serveur. Lorsque le datagramme arrive sur la première interface physique de la machine d'interconnexion, le protocole réseau fait que le datagramme remonte naturellement vers la couche applicative de la machine d'interconnexion, permettant ainsi à l'application relais de le capter.

Dans le cas où il est nécessaire de router par la machine d'interconnexion, les datagrammes transmis du réseau client au réseau serveur, le procédé est caractérisé en ce que la première étape est précédée d'une deuxième étape pour router les datagrammes transmis sur le réseau client à destination de la machine serveur, vers la machine d'interconnexion. C'est par exemple le cas lorsque la machine d'interconnexion entre le réseau client et le réseau serveur n'est pas unique.

D'autres avantages et détails de mise en œuvre de l'invention ressortent de la description qui suit en référence aux figures où:

- la figure 1 représente un exemple de machine d'interconnexion à deux interfaces physiques;
- la figure 2 représente un exemple de datagramme;
- la figure 3 représente un exemple de machine d'interconnexion à trois interfaces physiques.

Sur la figure 1 sont représentées des machines serveur 1, 2 et des machines client 11, 12. Les machines 1, 2, 11, sont reliées à un réseau serveur 3 au moyen d'interfaces physiques respectives 7, 8, 17. Une machine client 12 est reliée à un réseau client 13 au moyen d'une interface physique 18. Les réseaux 3 et 13 sont physiquement distincts. Une machine d'interconnexion 4 est reliée au réseau serveur 3 au moyen d'une interface physique 14 et au réseau 13 au moyen d'une interface physique 19.

Des applications 5, 6, 15, 16, exécutées dans les machines 1, 2, 11, 12, communiquent entre elles au moyen d'une couche transport CT selon un protocole en mode non connecté tel que UDP ou en mode connecté tel que TCP. La couche transport CT supervise une couche réseau CR selon un protocol tel que IP.

Dans la couche réseau CR, la machine 1 est reconnue au moyen d'une adresse @S1, la machine 2 est reconnue au moyen d'une adresse @S2, la machine 11 est reconnue au moyen d'une adresse @C1. De façon connue, chacune des adresses @S1, @S2 et @C1 possède un champ réseau avec une valeur commune qui identifie le réseau 3 et un champ machine avec une valeur distincte qui identifie chaque machine liée au réseau 3. La machine 12 est reconnue au moyen d'une adresse @C2 avec une valeur de champ réseau qui identifie le réseau 13 et une valeur de champ machine qui identifie la machine 12 sur le réseau 13. La machine 4 est reconnue au moyen d'une adresse @P1 avec une valeur de champ réseau qui identifie le réseau 13 et une valeur de champ machine qui identifie la machine 4 sur le réseau 13 et au moyen d'une adresse @P2 avec une valeur de champ réseau qui identifie le réseau 3 et une valeur de champ machine qui identifie la machine 4 sur le réseau 3.

Les machines communiquent entre elles au moyen de messages qui circulent sur les réseaux sous forme de datagrammes. La figure 2 présente un exemple de datagramme. Ce datagramme, constitué d'une trame de bits successifs, est structuré essentiellement en trois champs successifs. Un premier champ repéré DR est destiné au protocole de la couche réseau. Un deuxième champ repéré DT est destiné au protocole de la couche transport qui supervise la couche réseau. Un troisième champ repéré DA est destiné à une couche applicative qui supervise la couche transport. Dans le cas d'une requête sur la toile (web en anglais) par exemple, le champ DR contient les adresses IP source et destination, le champ DT contient les numéros de port TCP source et destination, le champ DA contient des données HTTP.

Par exemple, si une application client 15 exécutée dans la machine client 11, effectue une requête d'accès à un fichier traité par une application serveur 5 située dans la machine serveur 1, l'application 5 transmet sa requête à la couche CT de la machine 11 qui écrit la requête dans le champ DA et qui écrit dans le champ DT, un numéro de port de service pour l'application 15 et un numéro de port de service pour l'application 5. La couche CT de la machine 11 transmet les champs DT et DA à la couche CR de la machine 11 qui écrit dans le champ DR, l'adresse @C1 de la machine 11 et l'adresse @S1 de la machine 1. La couche CR transmet ensuite le datagramme ainsi constitué à l'interface 17 qui arrive sur l'interface 7 de la machine 1. La couche CR de la machine 1 reconnaît par l'adresse @S1 que le datagramme est destiné aux couches supérieures de la machine 1 et retransmet les champs DT et DA à la couche CT de la machine 1. Au moyen du numéro de port de service

pour l'application 5, la couche CT retransmet le champ DA à l'application 5 qui traite la requête.

Si une application 16 exécutée dans la machine client 12, effectue une requête d'accès à un fichier traité par l'application 5 située dans la machine serveur 1, l'application 16 transmet sa requête à la couche CT de la machine 12 qui l'écrit dans le champ DA et qui écrit dans le champ DT, un numéro de port de service pour l'application 16 et un numéro de port de service pour l'application 5. La couche CT de la machine 12 transmet les champs DT et DA à la couche CR de la machine 12 qui écrit dans le champ DR, l'adresse @C2 de la machine 12 et l'adresse @S1 de la machine 1. La couche CR transmet ensuite le datagramme ainsi constitué à l'interface 18 qui arrive sur l'interface 19 de la machine 4, déclarée comme routeur entre les réseaux 13 et 3.

En absence de dispositif selon l'invention, l'adresse @S1 n'étant pas une adresse de destination de la machine 4, la couche CR de la machine 4 reconnaît que le datagramme n'est pas destiné aux couches supérieures de la machine 4. La couche CR de la machine 4 recherche alors dans des tables de routage une ligne contenant une valeur identique au champ réseau de l'adresse @S1. La ligne ainsi trouvée indique alors l'interface 14 comme étant celle d'accès au réseau 3. La couche CR de la machine 4 retransmet alors le datagramme sur le réseau 3 par l'interface 14 de sorte que le datagramme arrive sur l'interface 7 de la machine 1. La couche CR de la machine 1 reconnaît par l'adresse @S1 que le datagramme est destiné aux couches supérieures de la machine 1 et retransmet les champs DT et DA à la couche CT de la machine 1. Au moyen du numéro de port de service pour l'application 5, la couche CT retransmet le champ DA à l'application 5 qui traite la requête.

Avec le dispositif selon l'invention, la machine 4 comprend une application 22 qui joue le rôle de relais (proxy server en anglais) pour des requêtes en provenance du réseau 13. L'application 22 présente plusieurs avantages, par exemple elle peut effectuer un contrôle d'accès aux machines 1, 2, 11 reliées au réseau serveur 3, elle peut sauvegarder des réponses à des requêtes précédentes dans une antémémoire (cache en anglais) pour restituer ces réponses à de nouvelles requêtes sans nécessiter d'acheminer ces nouvelles requêtes jusqu'à la machine serveur 1, 2.

Plusieurs adresses de la couche CR sont associées à l'interface physique 19, d'une part l'adresse habituelle @P1 et d'autre part l'adresse @S1 de la machine serveur 1 reliée au

réseau 3. Il est possible aussi d'associer l'adresse @S2 de la machine serveur 2 à l'interface physique 19. Comme il ressort de la suite de la description, à la différence de l'état de la technique où c'est le réseau client qui détermine l'utilisation des services de l'application relais 22, c'est ici le réseau serveur qui détermine cette utilisation par exemple l'accès au serveur 1 en associant l'adresse @S1 à l'interface physique 19.

L'application 22 comprend un port d'entrée 9 de numéro identique au port d'entrée de l'application 5 et un port de sortie 10 auquel elle a la possibilité d'attribuer un numéro pour gérer des messages de requête éventuels à destination de l'application 5.

Grâce à ce dispositif particulier, la machine 12 n'a pas besoin de savoir qu'elle établit une connexion intermédiaire avec la machine 4. Si une application 16 exécutée dans la machine client 12, effectue une requête destinée à l'application 5 située dans la machine serveur 1, l'adresse @S1 est maintenant reconnue sur le réseau 13 comme étant celle de la machine 4.

Pour effectuer une requête destinée à l'application 5, l'application 16 envoie un datagramme Q sur le réseau 13 qui contient dans le champ CR, les adresses @S1 et @C2, dans le champ transport, les numéros de port des applications 5 et 16, dans le champ CA, les informations finales destinées à l'application 5.

Lorsque le datagramme Q est reçu sur l'interface physique 19 de la machine 4, la couche réseau CR de la machine 4 reconnaît l'adresse de destination @S1 dans le champ DR comme étant une adresse qui lui est propre et remonte donc le datagramme vers la couche transport CT de la machine 4. La couche transport CT reconnaît le numéro de destination dans le champ DT comme étant le numéro du port 9 de l'application 22 à laquelle elle transmet alors le contenu du datagramme Q.

L'application 22 traite alors le contenu du champ DA du datagramme Q. Le traitement du datagramme Q par l'application 22 consiste par exemple à vérifier des droits d'accès, à vérifier si la machine 4 contient déjà une réponse à la requête dans son antémémoire pour décider de communiquer ou de ne pas communiquer le datagramme Q à l'application serveur 5.

Lorsque pour traiter le message de requête en provenance de l'application client 16, l'application 22 a besoin d'émettre un message de requête vers l'application 5, l'application

22 communique les données suivantes à la couche transport CT de la machine 4, le contenu de la requête à mettre dans le champ DA, le numéro de port d'entrée de l'application 5, un numéro de port de sortie de l'application 22 pour gérer la réponse à la requête, l'adresse protocolaire inter-réseau @S1 de la machine 1. Ces données sont transmises à la couche réseau CR de la machine 4. A réception de ces données, la couche réseau CR de la machine 4 recherche dans ses tables de routages sur quel réseau émettre un datagramme, en fonction du champ réseau de l'adresse @S1. Dans l'exemple ici décrit, le champ réseau de l'adresse @S1 correspondant au réseau 3 auquel est reliée la machine 1, la couche CR émet vers l'interface physique 14, un datagramme contenant dans le champ DR, l'adresse de destination @S1 et l'adresse source @P2 associée à l'interface physique 14. Sur le réseau serveur 3, le datagramme parvient de façon classique jusqu'à la machine 1 et jusqu'à l'application serveur 5 dans la machine 1.

La réponse reçue de l'application 5 sur l'interface 14 est remontée à l'application 22 par la couche réseau car l'adresse @P2 est une adresse de la machine 4, et par la couche transport CT car le numéro de port pour la réponse est celui attribué sur le port 10 par l'application 22. Au moyen d'un mécanisme interne de gestion de requêtes et de réponses, l'application 22 associe la réponse au numéro de port de sortie reçu de l'application 16. Pour réémettre la réponse vers l'application 16, l'application 22 communique les données suivantes à la couche transport CT de la machine 4, le contenu de la réponse à mettre dans le champ DA, le numéro de port de sortie de l'application 16, le numéro de port d'entrée de l'application 22 qui est identique au numéro de port d'entrée de l'application 5 pour gérer la réponse à la requête, l'adresse protocolaire inter-réseau de destination @C2 de la machine 12 et l'adresse protocolaire inter-réseau source @S1 de la machine 1. Ces données sont transmises à la couche réseau CR de la machine 4 par la couche transport. A réception de ces données, la couche réseau CR de la machine 4 recherche dans ses tables de routages sur quel réseau émettre un datagramme, en fonction du champ réseau de l'adresse @C2. Dans l'exemple ici décrit, le champ réseau de l'adresse @C2 correspondant au réseau 13 auquel est reliée la machine 12, la couche CR émet vers l'interface physique 19, un datagramme contenant dans le champ DR, l'adresse de destination @P2 et l'adresse source @S1 associée à l'interface physique 19. Sur le réseau client 13, le datagramme parvient de façon classique jusqu'à la machine 12 et jusqu'à l'application client 16 dans la machine 1.

Ainsi, l'application 16 dans la machine 12 voit revenir une réponse en provenance de l'application 5 dans la machine 1 sans voir son transit par l'application 22 qui s'est fait de façon transparente pour l'application client 16.

En référence à la figure 3, l'adresse @S1 est associée à une interface physique 20 différente tant de l'interface 14 comme précédemment que de l'interface 19 comme ici particulièrement.

Lorsqu'un datagramme est émis sur le réseau 13 avec l'adresse @S1, le protocole de routage de la couche réseau CR de la machine 4 le capte sur l'interface 19 à laquelle est associée l'adresse @P1. Comme l'adresse @S1 associée à l'interface physique 20, est une adresse de la machine 4, le datagramme est remonté à la couche applicative CA de la machine 4.

Une application relais 21 traite le message de requête issu du datagramme reçu, de façon identique à l'application relais 22 précédente. Pour émettre le message de réponse vers l'application 12, l'application relais 22 dispose d'un pilote particulier vers un réseau virtuel auquel est reliée l'interface physique 20.

Le cas où l'adresse IP @S1 est associée à l'interface 19 est particulièrement avantageuse pour la facilité de mise en œuvre de l'invention. Dans l'exemple simple qui suit, l'application 16 exécute une fonction Telnet en tant qu'application cliente, l'application 22 exécute une fonction telnetd en tant qu'application serveur de l'application 16 et une fonction Telnet en tant que client de l'application 5. L'application 5 exécute une fonction telnetd en tant que serveur de l'application 22. Telnet et telnetd sont des fonctions connues, utilisant TCP/IP pour connecter un terminal de machine client où s'exécute la fonction Telnet, à une machine serveur où s'exécute la fonction telnetd.

De façon à suivre sur quelle machine sont exécutées les commandes, chacune tourne sur un système d'exploitation différent. La machine client 12 tourne sur un système AIX (marque déposée) de version 4.1 et possède comme adresse IP: @C1 = 129.182.51.58. La machine relais 4 tourne sur un système AIX de version 4.2 et possède comme adresses IP: @P1 = 129.182.51.21 et @P2 = 192.90.249.22. La machine serveur 12 tourne sur un système DNS-E (propriétaire) et possède comme adresse IP: @S1 = 192.90.249.124. Le réseau 13 est accessible de façon connue par une adresse IP: @R1 = 129.182.50 avec un masque @M1 = 255.255.254.0.

Sur la machine client 12, la commande:

route add -host 192.90.249.124 129.182.51.21

définit que pour atteindre la machine serveur 1 d'adresse @S1, les datagrammes émis passent par la machine relais d'adresse @P1.

Sur la machine serveur 1, la commande:

route add -net 129.182.50 192.90.249.22 -netmask 255.255.254.0

définit que pour atteindre toute machine du réseau 13 d'adresse @R1, les datagrammes émis passent par la machine relais d'adresse @P2.

Sur la machine client 12, la commande:

Telnet 192.90.249.124

active l'application Telnet pour atteindre la machine serveur 1 d'adresse @S1. A ce stade, la seule machine reconnue par l'adresse IP @S1 est la machine serveur 1. La couche IP de la machine 4 route les datagrammes émis par la couche IP de la machine 12, vers la couche IP de la machine serveur 1. La couche IP de la machine 1 reconnaissant l'adresse @S1, remonte le champ applicatif des datagrammes vers l'application telnetd de la machine 1. L'application telnetd de la machine 1 émet en retour vers la machine 12, le message:

Trying...
Connected to 192.90.249.124.
Escape character is '^]'.
$$ 0000 *DNS-E V3U1.000 P1.001 P2.019 P3.010*IMA:BX77SIM 1998/10/21 17:23*

L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans l'environnement du système DNS, c'est à dire qu'on atteint directement la machine 1. La machine relais 4 n'a été traversée que pour réaliser le routage IP.

Sur la machine client 12, la commande:

Telnet 129.182.51.21

active l'application Telnet pour atteindre la machine relais 4 d'adresse @P1. La couche IP de la machine 4 reconnaissant l'adresse @P1, remonte le champ applicatif des datagrammes vers l'application telnetd de la machine 4. L'application telnetd de la machine 4 émet en retour vers la machine 12, le message:

Trying...

Connected to 129.182.51.21.
Escape character is '^]'.
Telnet (treize)
AIX Version 4
© Copyrights by IBM and by others 1982, 1996.
Login:

L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans l'environnement du système AIX, c'est à dire qu'on atteint la machine 4. Ceci permet de générer des commandes depuis le terminal de la machine 12 qui sont exécutées dans la machine 4.

Sur la machine 4, l'interface 19 étant nommée en1, la commande:

ifconfig en1 192.90.249.124 alias

définit l'adresse @S1 comme une adresse supplémentaire associée à l'interface 19. La machine 4 ne risque pas d'être confondue avec la machine 1 sur le réseau 13 par la couche IP, car celui-ci est physiquement distinct du réseau 3. De même, la commande:

ifconfig en1 192.90.249.125 alias

définirait l'adresse @S2 comme une adresse supplémentaire associée à l'interface 19.

Revenant sur la machine 12, la commande:

Telnet 192.90.249.124

active alors l'application Telnet avec un effet différent de celui décrit précédemment. Le message affiché sur le terminal de la machine 12 est:

Trying...
Connected to 129.182.51.21.
Escape character is '^]'.
Telnet (treize)
AIX Version 4
© Copyrights by IBM and by others 1982, 1996.
Login:

L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans l'environnement du système AIX de la machine 4. Bien qu'ayant demandé une connexion à l'application telnetd de la machine serveur 1 au moyen de l'adresse @S1, la commande a effectué une connexion à l'application telnetd de la machine 4. Ceci s'explique par le fait que la couche IP de la machine 4 reconnaît l'adresse @S1 comme une adresse de destination propre à la machine 4, sans tenir compte du routage vers le réseau 3. Ainsi, la

couche IP de la machine 4 remonte le champ applicatif des datagrammes reçus sur l'interface 19, vers l'application telnetd de la machine 4.

A présent sur la machine 4, la commande:

Telnet 192.90.249.124

active l'application Telnet pour atteindre la machine serveur 1 d'adresse @S1. A ce stade, la seule machine reconnue par l'adresse IP @S1 à partir de l'interface 14, est la machine serveur 1. La couche IP de la machine 1 reconnaissant l'adresse @S1, remonte le champ applicatif des datagrammes vers l'application telnetd de la machine 1. L'application telnetd de la machine 1 émet en retour vers l'application Telnet de la machine 4, le message:

Trying...
Connected to 192.90.249.124.
Escape character is '^]'.
$$ 0000 *DNS-E V3U1.000 P1.001 P2.019 P3.010*IMA:BX77SIM 1998/10/21 17:23*

Ce message est retransmis par l'application telnetd de la machine 4 vers l'application Telnet de la machine 12. L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans l'environnement du système DNS, c'est à dire qu'on atteint la machine 1. Cependant, le champ applicatif des datagrammes est remonté à la couche applicative de la machine relais 4, de façon transparente pour la machine 12.

Le procédé qui vient d'être expliqué au moyen d'une manipulation manuelle, peut être réalisé au moyen d'un programme exécuté par la couche applicative de la machine 4.

Les datagrammes à destination de la machine 1, passant par la couche IP de la machine 4, sont remontés dans la couche applicative de la machine 4 car l'adresse @S1 est associée à une interface physique de la machine 4. Pour éviter des conflits sur le réseau 3 avec la machine 1, il est préférable de ne pas associer l'adresse @S1 à l'interface 14. En référence à la figure 3, il est possible d'associer l'adresse @S1 à une autre interface physique que l'interface 19, par exemple à une interface physique 20.

Un exemple de traitement particulier par l'application 22 décrit ici, présente un avantage particulier. Dans le cas où des clés de cryptage sont associées à l'adresse @S1 pour chiffr r les requêtes en provenance et les réponses à destination de la machine 12, le décryptage des requêtes et le cryptage des réponses peut être assuré par la machine 4. Les données peuvent circuler décryptées sur le réseau serveur 3 sans risque. Ainsi, les

ressources de cryptage et décryptage peuvent être centralisées dans la machine 4 en laissant un maximum de ressources disponibles à la machine 1 pour ses fonctions de serveur. L'application 22 se charge aussi de recrypter les réponses avant de les émettre sur le réseau 13.

REVENDICATIONS:

1. Machine d'interconnexion (4) reliée à un réseau client (13) au moyen d'une première interface physique (19) et reliée à un réseau serveur (3) au moyen d'une deuxième interface physique (14), caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux (@S1, @S2) d'une machine serveur (1, 2) reliée au réseau serveur (3), distincte de la machine d'interconnexion (4), est associée à la première interface physique (19), et en ce qu'elle comprend une première application relais (22) pour recevoir des datagrammes destinés à la machine serveur (1, 2) depuis le réseau client (13) et pour émettre sur le réseau serveur (3) des datagrammes à destination de la machine serveur (1,2).

2. Machine d'interconnexion (4) reliée à un réseau client (13) au moyen d'une première interface physique (19) et reliée à un réseau serveur (3) au moyen d'une deuxième interface physique (14), caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux (@S1, @S2) d'une machine serveur (1, 2) reliée au réseau serveur (3), distincte de la machine d'interconnexion (4), est associée à une troisième interface physique (20), distincte de la première interface physique (19) et de la deuxième interface physique (14) et en ce qu'elle comprend une première application relais (22) pour recevoir des datagrammes destinés à la machine serveur (1, 2) depuis le réseau client (13) et pour émettre sur le réseau serveur (3) des datagrammes à destination de la machine serveur (1,2).

3. Machine d'interconnexion (4) selon la revendication 1, caractérisée en ce que ladite adresse (@S1, @S2) est associée à la première interface physique (19) en tant qu'adresse synonyme d'une adresse de base (@P1) de la machine (4) sur le réseau (13).

4. Procédé pour permettre de traiter au moyen d'une application relais (22) exécutée dans une machine d'interconnexion (4) entre un réseau client (13) et un réseau serveur (3), des datagrammes émis sur le réseau client (13) par une application client (16) à destination d'une machine serveur (1) d'adresse (@S1) sur le réseau serveur (3), distincte de la machine d'interconnexio (4), caractérisé en ce qu'il comprend une première étape qui associe ladite adresse (@S1) à une interface physique (19, 20) de la machine d'interconnexion (4) qui n'est pas reliée au réseau serveur (3), de sorte que l'application relais (22) capte les dits

datagrammes sans nécessiter de configurer ou d'informer ladite application client (16) à cette fin.

5. Procédé selon la revendication 4, caractérisé en ce que la première étape est précédée d'une deuxième étape pour router les datagrammes transmis sur le réseau client (13) à destination de la machine serveur (1), vers la machine d'interconnexion (4).

6. Machine d'interconnexion (4) selon la revendication 1 ou 2, caractérisée en ce que l'application (22) dispose de clés de cryptages de façon à transmettre déchiffrés sur le réseau 3, des messages chiffrés en provenance du réseau 13.

7. Machine d'interconnexion (4) selon la revendication 1 ou 2, caractérisée en ce que l'application (22) dispose de clés de cryptages de façon à transmettre chiffrés sur le réseau 13, des messages non chiffrés en provenance du réseau 3.

Fig.1

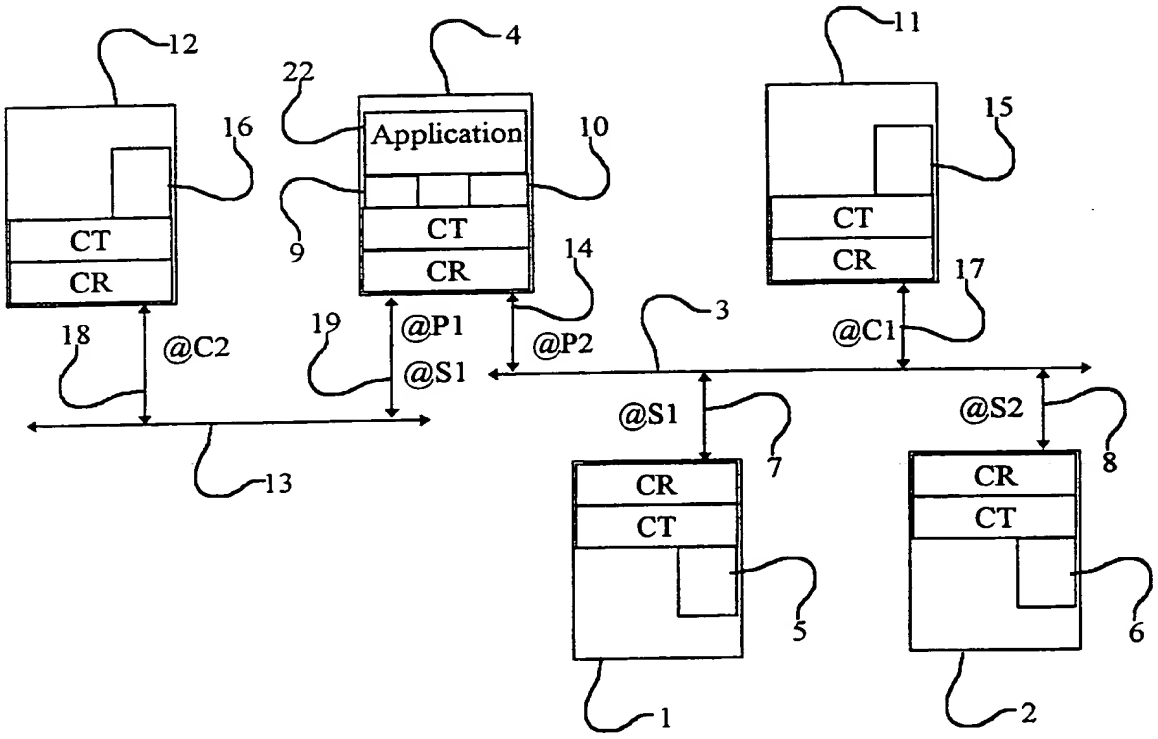


Fig.2

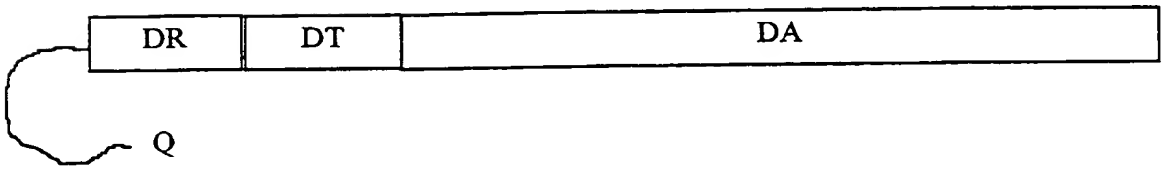
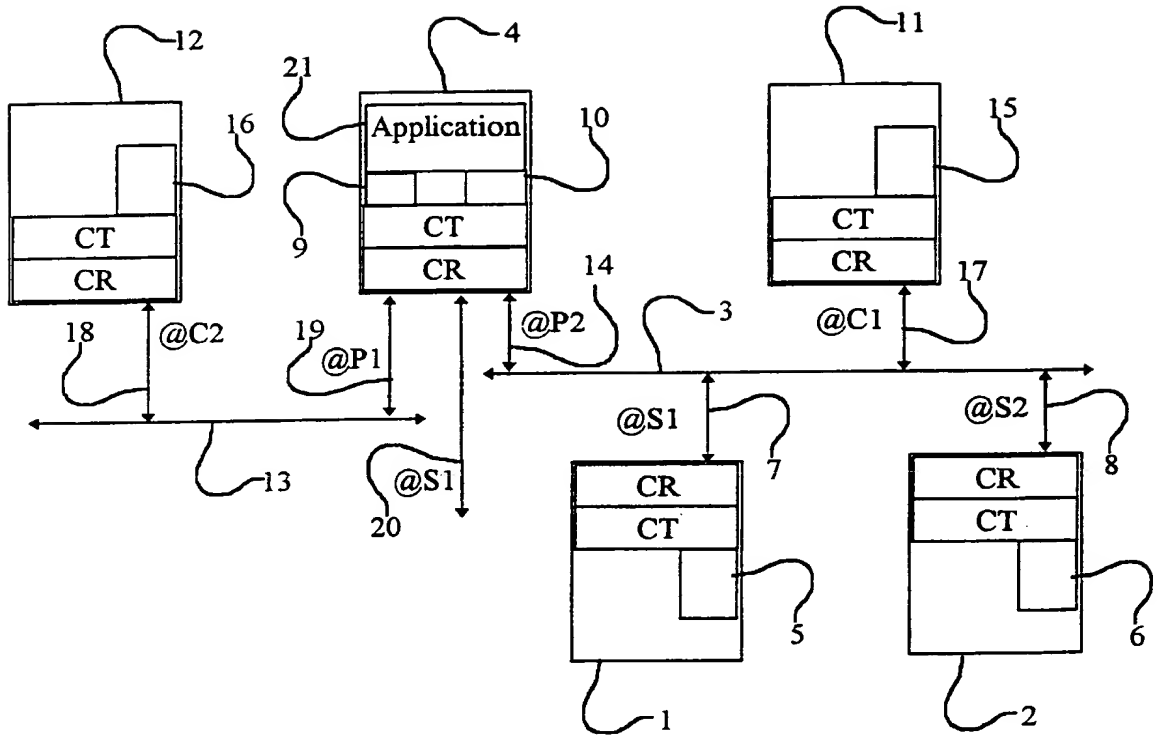


Fig.3



INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/FR 00/02469

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0 713 311 A (MILKYWAY NETWORKS CORP) 22 May 1996 (1996-05-22) page 4, line 48-58 page 6, line 16 -page 7, line 54 page 8, line 46-53 page 9, line 12-25	1,2 6,7
A Y	US 5 898 830 A (COLEY CHRISTOPHER D ET AL) 27 April 1999 (1999-04-27) column 4, line 17-52 column 7, line 41 -column 9, line 35 column 11, line 36 -column 12, line 27 column 14, line 66 -column 15, line 46	1,2,4 6,7

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 October 2000	20/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dupuis, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. ial Application No
PCT/FR 00/02469

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0713311 A	22-05-1996	CA 2136150 A	19-05-1996
		US 5623601 A	22-04-1997
US 5898830 A	27-04-1999	US 6052788 A	18-04-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Dema Internationale No
PCT/FR 00/02469

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 H04L29/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X Y	EP 0 713 311 A (MILKYWAY NETWORKS CORP) 22 mai 1996 (1996-05-22) page 4, ligne 48-58 page 6, ligne 16 -page 7, ligne 54 page 8, ligne 46-53 page 9, ligne 12-25	1,2 6,7
A Y	US 5 898 830 A (COLEY CHRISTOPHER D ET AL) 27 avril 1999 (1999-04-27) colonne 4, ligne 17-52 colonne 7, ligne 41 -colonne 9, ligne 35 colonne 11, ligne 36 -colonne 12, ligne 27 colonne 14, ligne 66 -colonne 15, ligne 46	1,2,4 6,7

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
13 octobre 2000	20/10/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dupuis, H

2

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 00/02469

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0713311 A	22-05-1996	CA 2136150 A	19-05-1996
		US 5623601 A	22-04-1997
US 5898830 A	27-04-1999	US 6052788 A	18-04-2000

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)